Please type a plus (+) inside this box →

PTO/SB/29 (12/97)
Approved for use through 09/30/00. OMB 0651-0032
Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

UTILITY PATENT APPLICATION TRANSMITTAL

(for new nonprovisional applications under 37 CFR 1.53(b))

Attorney Docket No.	9740-009-999	*Total Pages*	30
First Named Inventor or Application Identifier			
Joseph SILVESTER			
Express Mail Label No.	EM 061 021 962 US		

APPLICATION ELEMENTS

See MPEP chapter 600 concerning utility patent application contents.

1. ☒ Fee Transmittal Form [*Total Pages* 1+(1)]
   Submit an original, and a duplicate for fee processing)
2. ☒ Specification [*Total Pages* 19]
   (preferred arrangement set forth below)
   - -Descriptive title of the Invention
   - -Cross Reference to Related Applications
   - -Statement Regarding Fed sponsored R&D
   - -Reference to Microfiche Appendix
   - -Background of the Invention
   - -Brief Summary of the Invention
   - -Brief Description of the Drawings *(if filed)*
   - -Detailed Description of the Invention (including drawings, *if filed*)
   - -Claim(s)
   - -Abstract of the Disclosure
3. ☒ Drawing(s) *(35 USC 113)* [*Total Sheets* 7]
4. ☒ Oath or Declaration [*Total Sheets* 2]
   a. ☒ Newly executed (original or copy)
   b. ☐ Copy from a prior application (37 CFR 1.63(d))
   (for continuation/divisional with Box 17 completed)
   [Note Box 5 below]
   i. ☐ DELETION OF INVENTORS(S)
   Signed statement attached deleting inventor(s) named in the prior application, see 37 CFR 1.63(d)(2) and 1.33 (b).
5. ☐ Incorporation By Reference *(useable if Box 4b is checked)*
   The entire disclosure of the prior application, from which a copy of the oath or declaration is supplied under Box 4b, is considered as being part of the disclosure of the accompanying application and is hereby incorporated by reference therein.

ADDRESS TO: **Assistant Commissioner for Patents**
Box Patent Application
Washington, DC 20231

6. ☐ Microfiche Computer Program *(Appendix)*
7. ☐ Nucleotide and/or Amino Acid Sequence Submission *(if applicable, all necessary)*
   a. ☐ Computer Readable Copy
   b. ☐ Paper Copy (identical to computer copy)
   c. ☐ Statement verifying identity of above copies

ACCOMPANYING APPLICATION PARTS

8. ☒ Assignment Papers (cover sheet & document(s))
9. ☐ 37 CFR 3.73(b) Statement ☐ Power of Attorney
   (when there is an assignee)
10. ☐ English Translation Document *(if applicable)*
11. ☐ Information Disclosure Statement (IDS)/PTO-1449 ☐ Copies of IDS Citations
12. ☐ Preliminary Amendment
13. ☒ Return Receipt Postcard (MPEP 503)
    (Should be specifically itemized)
14. ☒ Small Entity ☐ Statement filed in prior application, Statement(s) Status still proper and desired
15. ☐ Certified Copy of Priority Document(s)
    (if foreign priority is claimed)
16. ☐ Other:

17. If a **CONTINUING APPLICATION**, *check appropriate box and supply the requisite information:*
☐ Continuation ☐ Divisional ☐ Continuation-in-part (CIP) of prior application No: filed.

18. CORRESPONDENCE ADDRESS

☒ Customer Number or Bar Code Label 20583 *(Insert Customer No. or Attach bar code label here)* or ☐ Correspondence address below

NAME					
ADDRESS					
CITY		*STATE*		*ZIP CODE*	
COUNTRY		*TELEPHONE*		*FAX*	

Burden Hour Statement: This form is estimated to take 0.2 hours to complete. Time will vary depending upon the needs of the individual case. Any comments on the amount of time you are required to complete this form should be sent to the Chief Information Officer, Patent and Trademark Office, Washington, DC 20231. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Assistant Commissioner for Patents, Box Patent Application, Washington, DC 20231.

Applicant or Patentee: SILVESTER, Joseph et al.
Serial or Patent No.: Attorney's docket No.: 9740-609-999
Filed or Issued:
For: **METHOD FOR THE SEPARATE AUTHENTICATION OF A TEMPLATE AND USER DATA**

VERIFIED STATEMENT (DECLARATION) CLAIMING SMALL ENTITY STATUS (37 CFR 1.9(f) and 1.27(c)) - SMALL BUSINESS CONCERN

I hereby declare that I am:

( ) the owner of the small business concern identified below:

(X) an official of the small business concern empowered to act on behalf of the concern identified below:

FULL NAME OF CONCERN SILANIS TECHNOLOGY INC.
ADDRESS OF CONCERN 3333 Côte Vertu, Suite 305, St-Laurent (Québec) H4R 2N1 CANADA

I hereby declare that the above identified small business concern qualifies as a small business concern as defined in 13 CFR 121.1301 through 121.1305, and reproduced in 37 CFR 1.9(d), for purposes of paying reduced fees to the United States Patent and Trademark Office, in that the number of employees of the concern, including those of its affiliates, does not exceed 500 persons. For purposes of this statement, (i) the number of employees of the business concern is the average over the previous fiscal year of the concern of the persons employed on a full-time, part-time or temporary basis during each of the pay periods of the fiscal year, and (2) concerns are affiliates of each other when either, directly or indirectly, one concern controls or has the power to control the other, or a third party or parties controls or has the power to control both.

I hereby declare that rights under contract or law have been conveyed to and remain with the small business concern identified above with regard to the invention, entitled

METHOD FOR THE SEPARATE AUTHENTICATION OF A TEMPLATE AND USER DATA

by inventor(s) SILVESTER, Joseph et al.
described in:
(X) the specification filed herewith
( ) application serial No., filed
( ) patent No. , issued

If the rights held by the above identified small business concern are not exclusive, each individual, concern or organization having rights in the invention is listed below* and no rights to the invention are held by any person, other than the inventor, who could not qualify as an independent inventor under 37 CFR 1.9(c) if that person made the invention, or by any concern which would not qualify as a small business concern under 37 CFR 1.9(d) or a nonprofit organization under 37 CFR 1.9(e).

*NOTE: Separate verified statements are required from each named person, concern or organization having rights to the invention averring to their status as small entities. (37 CFR 1.27)

FULL NAME
ADDRESS

( ) INDIVIDUAL ( ) SMALL BUSINESS CONCERN ( ) NONPROFIT ORGANIZATION

( ) See attached sheet for additional person(s), concern(s) or organization(s)

I acknowledge the duty to file, in this application or patent, notification of any change in status resulting in loss of entitlement to small entity status prior to paying, or at the time of paying, the earliest of the issue fee or any maintenance fee due after the date on which status as a small entity is no longer appropriate. (37 CFR 1.28(b)).

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that wilful false statements and the like so made are punishable by fine or imprisonment, or both, under section 1001 of Title 18 of the United States Code, and that such wilful false statements may jeopardize the validity of the application, any patent issuing thereon, or any patent to which this verified statement is directed.

NAME OF PERSON SIGNING: Tommy PETROGIANNIS
TITLE OF PERSON OTHER THAN OWNER PRESIDENT
ADDRESS OF PERSON SIGNING 4560 CUMBERLAND, MONTREAL PQ, H4B 2L4
SIGNATURE
Date Sept. 22, 1999

METHOD FOR THE SEPARATE AUTHENTICATION OF A TEMPLATE AND USER DATA

FIELD OF THE INVENTION

The present invention relates to the secure handling of data and more particularly concerns a method for separately authenticating a template and user data inserted in the template.

BACKGROUND OF THE INVENTION

There are many computer systems that have been designed to create, store, approve, revise or verify data electronically. Many of the documents that have been created through these systems have relied on a pre-existing template as a means of assembling data. This facilitates the means of data entry and allows the user to store the data and the template on one document. The use of the template also contributes to a less time-consuming process of entering information on an electronic document, a process that may contribute to fewer costs than those associated with paper-based data collection.

While there exist a great number of systems that may facilitate the creation, serial approval, storage and authentication of documents or of templates, there is no known system to date that can enable users to separate user data from template information. Current systems allow users to create templates and enter data in them. The data therefore becomes bound to the template in a single document. However, such systems do not have the capacity to enable users to securely approve, store and authenticate each portion separately, to approve multiple templates or, alternatively, opt to recreate the complete document.

Existing systems vary in the scope of the functions they can perform. Some are particularly limited, such as U.S. patent no. 4,933,969 to

Marshall et al., which primarily addresses authentication and storage. This mechanism stores information and protects against unauthorized modifications. While this type of data authentication system contributes greatly to ensuring the security and integrity of data, it lacks the capacity for the generation, approval and secure storage of both template information and user data.

Other systems offer certain types of electronic functions that are related to the generation and authentication of electronic signatures. For example, U.S. patent no. 5,195,133 to Kapp et al. describes a system designed to generate a completed payment document, which can be signed by a customer, and then capture that customer's signature in digital form. The principal feature of this mechanism is that it seeks to ensure that a signature approving a particular document was, in fact, captured at the time of the completion of the transaction to which it relates and was not obtained on some other occasion and merely reproduced for the particular transaction in question. The Kapp et al. patent creates a digital record of the transaction and captures a digital representation of the signature at the time the transaction is completed. This system then uses this digital record to encrypt the digital representation of the signature. However, it does not offer any possibility of generating or approving a template document separately from the user data or the electronic approval.

Other technology provides for the creation of an electronic signature for a particular signer only, and cannot be used for any document other than the one for which the signature was given (U.S. patent no. 5,689,567). U.S. patent no. 5,606,609 to Houser and Adler is a system designed to verify the integrity or signer of electronic documents. This is accomplished by embedding and encrypting security information in the electronic document at a location selected by the signer. When the electronic document is subsequently displayed, the technology decrypts the security information and verifies the identity of the signer. In another mechanism,

another method operates to authenticate and verify users on a network (U.S. patent no. 5,706,427). The possible applications of any of the aforementioned systems, albeit useful for certain purposes, are nonetheless limited as they do not allow for the creation, approval or authentication of template information distinct from the user data.

While each of the aforementioned systems can be useful for electronic business processes, they all have certain deficiencies. These mechanisms lack the capacity to enable the user to generate, approve, store and authenticate template information separately from user data, with the possibility of subsequently merging the two later in a complete document. Current technology operates such that any user data entered on the template becomes bound to the template in one document. The present invention allows users to access either the template data, multiple templates and/or the user data as independent files. Moreover, the technology ensures that no unauthorized modifications can be made to either file or to the complete document. This therefore accords the user greater flexibility in accessing each file without compromising the security or authenticity of the data.

The Remote Template Approval ("RTA") can serve as a vital tool facilitating electronic business processes. Many industries, such as insurance for example, which rely on templates and standard forms as a means of gathering information or selling and marketing services can greatly benefit from this technology. The RTA would enable those marketing these services to securely store and access user data separately from the templates, while individual template information could be generated, accessed or modified for each subsequent user or purchaser. This would represent an efficient way of gathering, storing and authenticating client and template information. In addition, it would offer an easy and secure medium through which users or consumers could submit information and purchase services on-line.

Clearly then, as electronic business transactions become even more prevalent, the need to generate and store template information and user data as separate entities will become more pronounced as well. As this occurs, the need for the Remote Template Approval mechanism will expand with it.

SUMMARY OF THE INVENTION

The present invention provides a system and method designed to facilitate remote template approval. This system will enable users to separate user data from template information and authenticate and verify each portion separately. Thus, by virtue of this method, users will be able to approve template information separately from the data added to the template. Preferably, this invention will also enable users to securely recreate the complete document composed of both data and template and verify its authenticity. Such a process would represent a marked improvement over existing systems which enable users to add data to existing templates in such a fashion as to bind the data to the template in one document. The present invention allows the user to securely access the template and the data as distinct records, or to, optionally, access the complete document.

Accordingly, the present invention provides a method for the separate authentication of a template and of user data inserted therein, comprising the steps of:

a) providing the template, said template having a corresponding template ID and template Document Authentication Code, hereinafter referred to as DAC(t), linked thereto;

b) inserting the user data in the template;

c) extracting the user data from the template;

d) generating a user data Document Authentication Code, hereinafter referred to as DAC(d), based on the user data; and

e) storing the template ID, DAC(t), the user data and DAC(d) in an Approval Data Packet, hereinafter referred to as ADP.

There is also provided a method for the separate authentication of a template having entry fields and user data inserted into said fields, comprising the steps of:

a) selecting a template ID and a corresponding template Document Authentication Code, hereinafter referred to as DAC(t), linked to the template;

b) entering the user data;

c) linking the user data to the fields of the template;

d) generating a user data Document Authentication Code, hereinafter referred to as DAC(d), based on the user data; and

e) storing the template ID, DAC(t), the user data and DAC(d) in an Approval Data Packet, hereinafter referred to as ADP.

The present invention further provides a method for the separate authentication of a template and of user data inserted therein, comprising the steps of:

a) providing the template, said template having a corresponding template ID and template Document Authentication Code, hereinafter referred to as DAC(t), linked thereto;

b) inserting the user data in the template;

c) generating a complete document Document Authentication Code, hereinafter referred to as DAC(c), based on the template with the user data therein;

d) extracting the user data from the template;

e) generating a user data Document Authentication Code, hereinafter referred to as DAC(d), based on the user data; and

f) storing the template ID, DAC(t), the user data, DAC(c) and DAC(d) in an Approval Data Packet, hereinafter referred to as ADP.

Also provided is a method for the separate authentication of a template and of user data inserted therein by multiple users, comprising the steps of:

a) authenticating a template and user data from a first user according to the last method described above; and

b) for each subsequent user of the multiple users, performing the substeps of:

i) retrieving the template and DAC(c);

ii) inserting user data from previous users in the template;

iii)generating for the template with the user data from previous users therein a new complete document Document Authentication Code, hereinafter referred to as DAC(nc);

iv) comparing DAC(nc) with DAC(c), and proceeding only if DAC(nc) is equal to DAC(c);

v) inserting data from the current user in the template;

vi) generating a DAC(c), based on the template with the user data from the previous users and current user therein;

vii) extracting the user data from the previous users and current user from the template;

viii) generating a DAC(d), based on the user data extracted in step vii); and

ix) storing the user data, DAC(c) and DAC(d) in ADP.

The present invention can have numerous applications. For example, it could enable users to create and approve one document on one system (e-mail for example), with the target template indicated in the ADP, and send it to another system, which may be the same system or a completely different one. The message can then be entered into the actual template document with all the proper formatting and no need to convert the document.

This invention would be useful for many industries that rely on templates as a means of collecting data. The same template could be generated for each new user and the data collected could be stored separately or could also be combined with the template to create a completed document. This method would allow users to re-generate the template for each subsequent user.

The present invention and its advantages will be better understood upon reading the following non-restrictive description of embodiments thereof with reference to the accompanying drawings.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1 is a flow chart representing the main steps of a method for the separate authentication of a template and of user data inserted therein in accordance with a preferred embodiment of the present invention.

FIG. 2 is a flow chart detailing step f of the method of FIG. 1.

FIG. 3 is a flow chart representing the main steps of a method for the separate authentication of a template and of user data inserted therein in accordance with an alternative embodiment of the invention.

FIG. 4 is a flow chart representing the main steps of a method for the separate authentication of a template and of user data inserted therein in accordance with another embodiment of the invention.

FIG. 5 is a flow chart detailing step g of the method of FIG. 4.

FIG. 6 is a flow chart detailing another variant for step g of the method of FIG. 4.

FIG. 7 is a flow chart representing the main steps of a method for the separate authentication of a template and of user data inserted therein in accordance with yet another embodiment of the invention.

DESCRIPTION OF PREFERRED EMBODIMENTS OF THE INVENTION

Referring to FIGs. 1 and 2, the steps of a method for the separate authentication of a template and user data inserted in the template are shown. This method allows the secure handling of the template and user data independently, without having to store the user data inside the template.

The first step a) of the method of FIG. 1 consists of providing the template itself. A template ID, identifying the particular template chosen and a template Document Authentication code, DAC(t), are both linked to the template. DAC(t) is a code characterizing precisely the template's content, and is preferably generated through a one-way hash function. If the template is not pre-existing, step a) may include the substep of generating the template, creating the template ID and DAC(t) and storing the last two in an appropriate location, which can for example be inside the template itself or in a linked storage system.

The second step b) consists of inserting the user data in the template. The term "user data" is understood as encompassing any relevant information that may be entered in a template, including a user signature and the date of signing. The method may therefore be used in the context of the remote approval of a document. The template preferably has specific fields where the user data may be received.

The user data is then extracted from the template in accordance with step c), and in the next step d) a user data Authentication Code (DAC(c)) is generated, based on the user data itself independently of the template.

Step e) consists of storing the template ID, DAC(t), the user data and DAC(c) in an Approval Data Packet (ADP) which may be encrypted for security. The user data may alternatively be stored elsewhere and a link to its location may be provided in the ADP.

Referring to FIGS. 1 and 2, there is shown an optional step f) of reconstructing a complete document including both the template and the

user data. In accordance with this additional step, the template ID and DAC(t) are first retrieved from the ADP, and the template corresponding to the template ID is accessed and opened. A new DAC (DAC(nt)) is generated on the opened template, and compared to DAC(t). Corrective action is to be taken if they don't match. If they do match, the user data and DAC(d) are also retrieved. A DAC(nd) is generated on the user data and compared to DAC(d). If they also match, the user data may then be inserted in the template.

In an alternate embodiment of the invention, illustrated in FIG. 3, the method described above may be performed without actually accessing the template. In this embodiment, a template ID and the corresponding DAC(t) are selected, and the user data is entered, preferably in answer to prompts for particular information. The user data entered is then linked to corresponding fields in the template, so that a complete document including both the template and the user data may later be reconstructed.

Referring to FIGs. 4, 5 and 6, there is shown yet another embodiment of the invention. In this particular embodiment, a step is added between steps b) and c) of FIG. 1 where a DAC(c) is generated based on the template with the user data therein, before the user data is extracted from the template. This DAC(c) is stored in the ADP with the other relevant information. In this manner, when reconstructing the complete document, additional substeps of generating a DAC(nc) on the complete document once the user data is inserted in the template and comparing this DAC(nc) with DAC(c) may be performed, as shown in FIG. 5. Alternatively, only the DACs of the complete documents may be compared, completely bypassing the verifications of the separate template and user data, as illustrated in FIG. 6.

Referring to FIG. 7, there is shown another embodiment of the invention where multiple users insert user data sequentially in a single template. The method includes the steps of:

a) authenticating a template and user data from a first user according to the method of FIG. 4. In this manner, an ADP is created containing the template ID, DAC(t), the user data, DAC(d) and DAC(c).

b) for each subsequent user of the multiple users, the following substeps are performed:

i) retrieving the template and DAC(c) from the ADP;

ii) inserting user data from previous users in the template. The document thereby generated corresponds to the complete document of the previous iteration;

iii)generating for the template with the user data from previous users therein a new complete document Document Authentication Code (DAC(nc));

iv) comparing DAC(nc) with DAC(c), and proceeding only if DAC(nc) is equal to DAC(c);

v) inserting data from the current user in the template;

vi) generating a DAC(c), based on the template with the user data from the previous users and current user therein;

vii) extracting the user data from the previous users and current user from the template;

viii) generating a DAC(d), based on the user data extracted in step vii); and

ix) storing the user data, DAC(c) and DAC(d) in ADP. DAC(c) and DAC(d) thereby replace the previously stored values of these variables.

An additional step of reconstructing the complete document, which in this case corresponds to the document generated in the last iteration of step b), may also be performed, either in the manner illustrated in FIG. 5 or FIG. 6.

Of course, numerous changes could be made to the preferred embodiment disclosed hereinabove without departing from the scope of the invention as defined in the appended claims.

WHAT IS CLAIMED IS:

1. A method for the separate authentication of a template and of user data inserted therein, comprising the steps of:

a) providing the template, said template having a corresponding template ID and template Document Authentication Code, hereinafter referred to as DAC(t), linked thereto;

b) inserting the user data in the template;

c) extracting the user data from the template;

d) generating a user data Document Authentication Code, hereinafter referred to as DAC(d), based on the user data; and

e) storing the template ID, DAC(t), the user data and DAC(d) in an Approval Data Packet, hereinafter referred to as ADP.

2. The method according to claim 1, wherein step a) comprises the substeps of:

i) generating the template;

ii) creating the template ID;

iii) creating DAC(t); and

iv) storing the template ID and DAC(t) in a location linked to the template.

3. The method according to claim 2, wherein substep a)iii) comprises generating DAC(t) from a one-way hash function.

4. The method according to claim 2, wherein, in substep a) iv), the location linked to the template is inside said template.

5. The method according to claim 2, wherein, in substep a) iv), the location linked to the template is a linked storage system.

6. The method according to claim 1, wherein step e) further comprises encrypting the ADP.

7. The method according to claim 1, further comprising an additional step f) of reconstructing an authenticated complete document, said complete document including the template and the user data.

8. The method according to claim 7, wherein step f) comprises the substeps of:

i) retrieving the template ID and DAC(t) from the ADP;

ii) opening the template corresponding to said template ID;

iii) generating for said template a new template Document Authentication Code, hereinafter referred to as DAC(nt);

iv) comparing DAC(nt) with DAC(t), and proceeding only if DAC(nt) is equal to DAC(t);

v) retrieving the user data and DAC(d) from the ADP;

vi) generating for said user data a new user data Document Authentication Code, hereinafter referred to as DAC(nd);

vii) comparing DAC(nd) with DAC(d), and proceeding only if DAC(nd) is equal to DAC(d); and

viii) inserting the user data in the template.

9. A method for the separate authentication of a template having entry fields and user data inserted into said fields, comprising the steps of:

a) selecting a template ID and a corresponding template Document Authentication Code, hereinafter referred to as DAC(t), linked to the template;

b) entering the user data;

c) linking the user data to the fields of the template;

d) generating a user data Document Authentication Code, hereinafter referred to as DAC(d), based on the user data; and

e) storing the template ID, DAC(t), the user data and DAC(d) in an Approval Data Packet, hereinafter referred to as ADP.

10. The method according to claim 9, wherein step b) further comprises prompting the user for the user data.

11. The method according to claim 9, wherein step e) further comprises encrypting the ADP.

12. The method according to claim 9, further comprising an additional step f) of reconstructing an authenticated complete document, said complete document including the template and the user data.

13. The method according to claim 12, wherein step f) comprises the substeps of:

i) retrieving the template ID and DAC(t) from the ADP;

ii) opening the template corresponding to said template ID;

iii) generating for said template a new template Document Authentication Code, hereinafter referred to as DAC(nt);

iv) comparing DAC(nt) with DAC(t), and proceeding only if DAC(nt) is equal to DAC(t);

v) retrieving the user data and DAC(d) from the ADP;

vi) generating for said user data a new user data Document Authentication Code, hereinafter referred to as DAC(nd);

vii) comparing DAC(nd) with DAC(d), and proceeding only if DAC(nd) is equal to DAC(d); and

viii) inserting the user data in the template.

14. A method for the separate authentication of a template and of user data inserted therein, comprising the steps of:

a) providing the template, said template having a corresponding template ID and template Document Authentication Code, hereinafter referred to as DAC(t), linked thereto;

b) inserting the user data in the template;

c) generating a complete document Document Authentication Code, hereinafter referred to as DAC(c), based on the template with the user data therein;

d) extracting the user data from the template;

e) generating a user data Document Authentication Code, hereinafter referred to as DAC(d), based on the user data; and

f) storing the template ID, DAC(t), the user data, DAC(c) and DAC(d) in an Approval Data Packet, hereinafter referred to as ADP.

15. The method according to claim 14, wherein step a) comprises the substeps of:

i) generating the template;

ii) creating the template ID;

iii) creating DAC(t); and

iv) storing the template ID and DAC(t) in a location linked to the template.

16. The method according to claim 15, wherein substep a)iii) comprises generating DAC(t) from a one-way hash function.

17. The method according to claim 15, wherein, in substep a) iv), the location linked to the template is inside said template.

18. The method according to claim 15, wherein, in substep a) iv), the location linked to the template is a linked storage system.

19. The method according to claim 14, wherein step f) further comprises encrypting the ADP.

20. The method according to claim 14, further comprising an additional step g) of reconstructing an authenticated complete document, said complete document including the template and the user data.

21. The method according to claim 20, wherein step g) comprises the substeps of:

i) retrieving the template ID, DAC(t) and DAC(c) from the ADP;

ii) opening the template corresponding to said template ID;

iii) generating for said template a new template Document Authentication Code, hereinafter referred to as DAC(nt);

iv) comparing DAC(nt) with DAC(t), and proceeding only if DAC(nt) is equal to DAC(t);

v) retrieving the user data and DAC(d) from the ADP;

vi) generating for said user data a new user data Document Authentication Code, hereinafter referred to as DAC(nd);

vii) comparing DAC(nd) with DAC(d), and proceeding only if DAC(nd) is equal to DAC(d);

viii) inserting the user data in the template;

ix) generating for the template with the user data therein a new complete document Document Authentication Code, hereinafter referred to as DAC(nc); and

x) comparing DAC(nc) with DAC(c), and proceeding only if DAC(nc) is equal to DAC(c).

22. The method according to claim 20, wherein step g) comprises the substeps of:

i) retrieving the template ID, the user data and DAC(c) from the ADP;

ii) opening the template corresponding to said template ID;

iii) inserting the user data in the template;

iv) generating for the template with the user data therein a new complete document Document Authentication Code, hereinafter referred to as DAC(nc); and

v) comparing DAC(nc) with DAC(c), and proceeding only if DAC(nc) is equal to DAC(c).

23. A method for the separate authentication of a template and of user data inserted therein by multiple users, comprising the steps of:

a) authenticating a template and user data from a first user according to the method of claim 14; and

b) for each subsequent user of the multiple users, performing the substeps of:

i) retrieving the template and DAC(c);

ii) inserting user data from previous users in the template;

iii)generating for the template with the user data from previous users therein a new complete document Document Authentication Code, hereinafter referred to as DAC(nc);

iv) comparing DAC(nc) with DAC(c), and proceeding only if DAC(nc) is equal to DAC(c);

v) inserting data from the current user in the template;

vi) generating a DAC(c), based on the template with the user data from the previous users and current user therein;

vii) extracting the user data from the previous users and current user from the template;

viii) generating a DAC(d), based on the user data extracted in step vii); and

ix) storing the user data, DAC(c) and DAC(d) in ADP.

24. The method according to claim 23, further comprising an additional step c) of reconstructing an authenticated complete document, said complete document including the template and the user data from all of the multiple users.

25. The method according to claim 24, wherein step c) comprises the substeps of:

i) retrieving the template ID, DAC(t) and DAC(c) from the ADP;

ii) opening the template corresponding to said template ID;

iii) generating for said template a new template Document Authentication Code, hereinafter referred to as DAC(nt);

iv) comparing DAC(nt) with DAC(t), and proceeding only if DAC(nt) is equal to DAC(t);

v) retrieving the user data and DAC(d) from the ADP;

vi) generating for said user data a new user data Document Authentication Code, hereinafter referred to as DAC(nd);

vii) comparing DAC(nd) with DAC(d), and proceeding only if DAC(nd) is equal to DAC(d);

viii) inserting the user data in the template;

ix) generating for the template with the user data therein a new complete document Document Authentication Code, hereinafter referred to as DAC(nc); and

x) comparing DAC(nc) with DAC(c), and proceeding only if DAC(nc) is equal to DAC(c).

ABSTRACT

A method for the separate authentication of a template and of data inserted therein. A template is provided with a template ID and a template Data Authentication Code (DAC(t)). User data is inserted in the template, and then extracted to be handled separately. A DAC(d) is generated on the user data by itself, and stored in an Approval Data packet with the template ID, DAC(t) and the user data. The complete document with the template and the user data can later be reconstructed. The method may be useful for many industries that rely on templates as a means for collecting data.

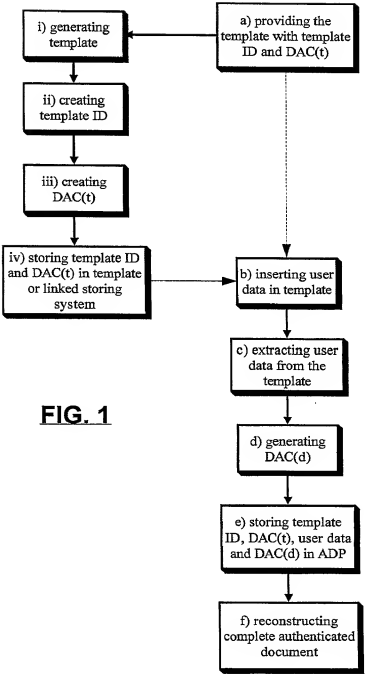
a) providing the template with template ID and DAC(t)
i) generating template
ii) creating template ID
iii) creating DAC(t)
iv) storing template ID and DAC(t) in template or linked storing system
b) inserting user data in template
c) extracting user data from the template
d) generating DAC(d)
e) storing template ID, DAC(t), user data and DAC(d) in ADP
f) reconstructing complete authenticated document

FIG. 1

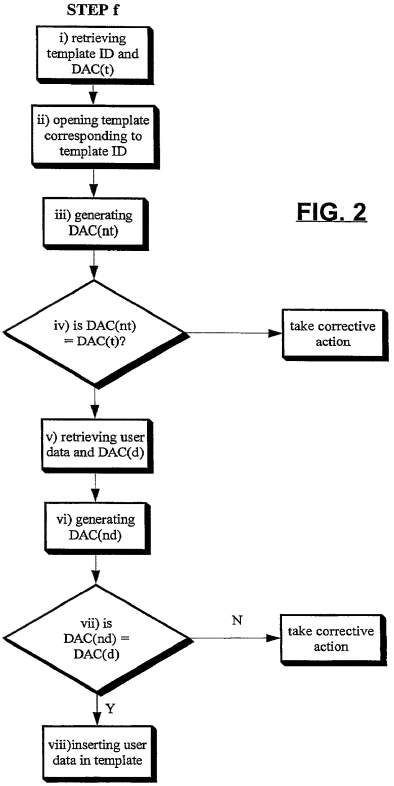
STEP f
i) retrieving template ID and DAC(t)
ii) opening template corresponding to template ID
iii) generating DAC(nt)
iv) is DAC(nt) = DAC(t)?
take corrective action
v) retrieving user data and DAC(d)
vi) generating DAC(nd)
vii) is DAC(nd) = DAC(d)
N
take corrective action
Y
viii)inserting user data in template

FIG. 2

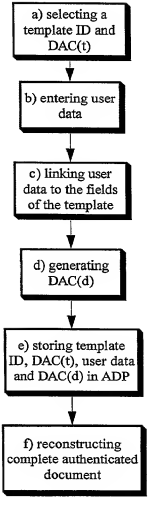

FIG. 3

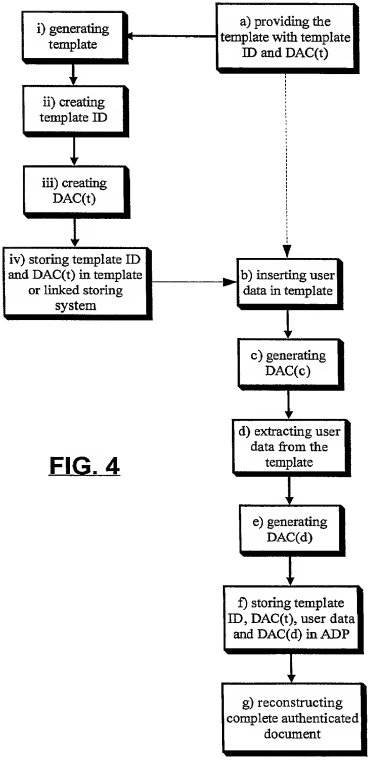
i) generating template
a) providing the template with template ID and DAC(t)
ii) creating template ID
iii) creating DAC(t)
iv) storing template ID and DAC(t) in template or linked storing system
b) inserting user data in template
c) generating DAC(c)
d) extracting user data from the template
e) generating DAC(d)
f) storing template ID, DAC(t), user data and DAC(d) in ADP
g) reconstructing complete authenticated document

FIG. 4

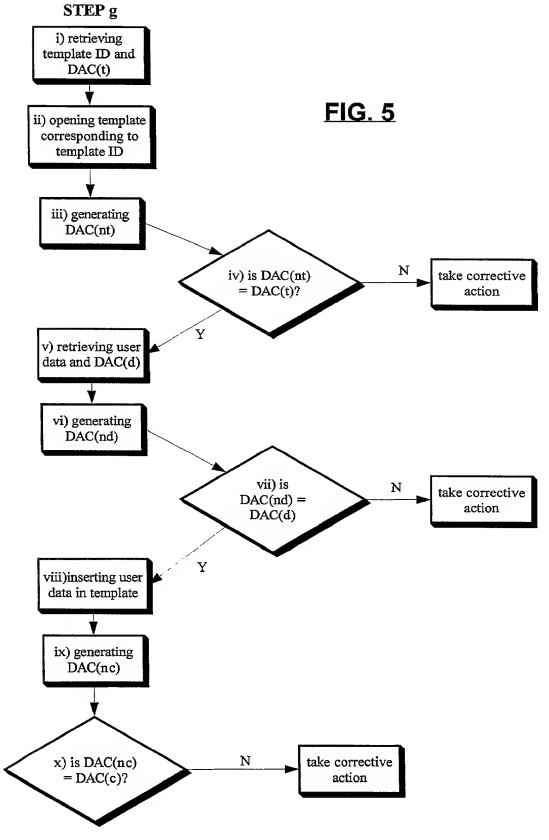
STEP g
i) retrieving template ID and DAC(t)
ii) opening template corresponding to template ID
iii) generating DAC(nt)
iv) is DAC(nt) = DAC(t)?
N
take corrective action
Y
v) retrieving user data and DAC(d)
vi) generating DAC(nd)
vii) is DAC(nd) = DAC(d)
N
take corrective action
Y
viii)inserting user data in template
ix) generating DAC(nc)
x) is DAC(nc) = DAC(c)?
N
take corrective action

FIG. 5

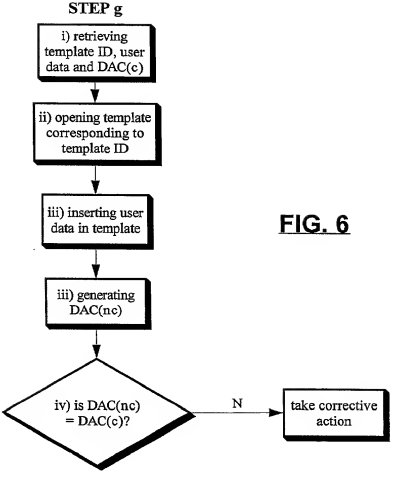
STEP g
i) retrieving template ID, user data and DAC(c)
ii) opening template corresponding to template ID
iii) inserting user data in template
iii) generating DAC(nc)
iv) is DAC(nc) = DAC(c)?
N
take corrective action

FIG. 6

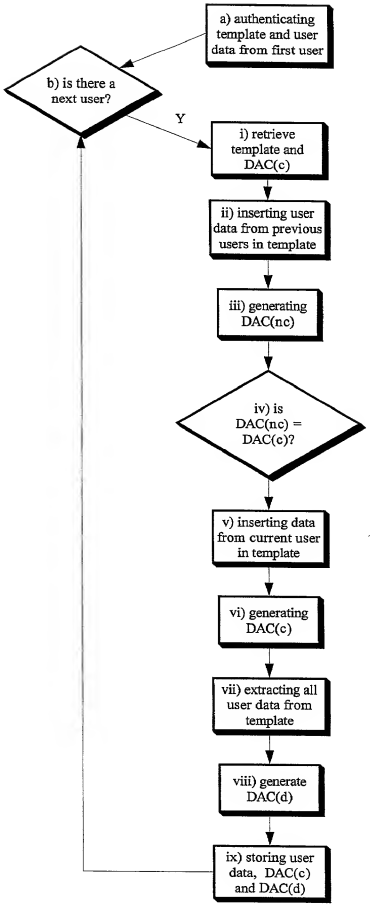
a) authenticating template and user data from first user
b) is there a next user?
Y
i) retrieve template and DAC(c)
ii) inserting user data from previous users in template
iii) generating DAC(nc)
iv) is DAC(nc) = DAC(c)?
v) inserting data from current user in template
vi) generating DAC(c)
vii) extracting all user data from template
viii) generate DAC(d)
ix) storing user data, DAC(c) and DAC(d)

FIG. 7

PENNIE & EDMONDS LLP DOCKET NO. 9740-009-999

DECLARATION AND POWER OF ATTORNEY

As a below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below at 201 et seq. underneath my name.

I believe I am the original, first and sole inventor if only one name is listed at 201 below, or an original, first and joint inventor if plural names are listed at 201 et seq. below, of the subject matter which is claimed and for which a patent is sought on the invention entitled

METHOD FOR THE SEPARATE AUTHENTICATION OF A TEMPLATE AND USER DATA

and for which a patent application:
☒ is attached hereto ~~and includes amendment(s) filed on~~ ______ *(if applicable)*
☐ was filed in the ~~United States on~~ ______ as Application No. ______ *(for declaration not accompanying application)*
with amendment(s) filed on ______ *(if applicable)*
☐ was filed as PCT international Application No. ______ on ______ and was amended under PCT Article 19 on *(if applicable)*

I hereby state that I have reviewed and understand the contents of the above identified application, including the claims, as amended by any amendment referred to above.

I acknowledge the duty to disclose information known to me to be material to patentability as defined in Title 37, Code of Federal Regulations, §1.56.

I hereby claim foreign priority benefits under Title 35, United States Code, §119(a)-(d) of any foreign application(s) for patent or inventor's certificate listed below and have also identified below any foreign application for patent or inventor's certificate having a filing date before that of the application on which priority is claimed:

EARLIEST FOREIGN APPLICATION(S), IF ANY, FILED PRIOR TO THE FILING DATE OF THE APPLICATION			
APPLICATION NUMBER	COUNTRY	DATE OF FILING (day, month, year)	PRIORITY CLAIMED
2,246,006	CANADA	25.09.98	YES ☒ NO ☐
			YES ☐ NO ☐

I hereby claim the benefit under Title 35, United States Code, §119(e) of any United States provisional application(s) listed below.

APPLICATION NUMBER	FILING DATE

I hereby claim the benefit under Title 35, United States Code, §120 of any United States application(s) listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States application in the manner provided by the first paragraph of Title 35, United States Code §112, I acknowledge the duty to disclose information which is material to patentability as defined in Title 37, Code of Federal Regulations, §1.56 which became available between the filing date of the prior application and the national or PCT international filing date of this application:

APPLICATION SERIAL NO.	FILING DATE	STATUS		
		PATENTED	PENDING	ABANDONED

POWER OF ATTORNEY: As a named inventor, I hereby appoint S. Leslie Misrock (Reg. No. 18872), Harry C. Jones, III (Reg. No. 20280), Berj A. Terzian (Reg. No. 20060), Gerald J. Flintoft (Reg. No. 20823), David Weild, III (Reg. No. 21094), Jonathan A. Marshall (Reg. No. 24614), Barry D. Rein (Reg. No. 22411), Stanton T. Lawrence, III (Reg. No. 25736), Charles E. McKenney (Reg. No. 22795), Philip T. Shannon (Reg. No. 24278), Francis E. Morris (Reg. No. 24615), Charles E. Miller (Reg. No. 24576), Gidon D. Stern (Reg. No. 27469), John J. Lauter, Jr. (Reg. No. 27814), Brian M. Poissant (Reg. No. 28462), Brian D. Coggio (Reg. No. 27624), Rory J. Radding (Reg. No. 28749), Stephen J. Harbulak (Reg. No. 29166), Donald J. Goodell (Reg. No. 19766), James N. Palik (Reg. No. 25510), Thomas E. Friebel (Reg. No. 29258), Laura A. Coruzzi (Reg. No. 30742), Jennifer Gordon (Reg. No. 30753), Jon R. Stark (Reg. No. 30111), Allan A. Fanucci (Reg. No. 30256), Geraldine F. Baldwin (Reg. No. 31232), Victor N. Balancia (Reg. No. 31231), Samuel B. Abrams (Reg. No. 30605), Steven I. Wallach (Reg. No. 35402), Marcia H. Sundeen (Reg. No. 30893), Paul J. Zegger (Reg. No. 33821), Edmond R. Bannon (Reg. No. 32110), Bruce J. Barker (Reg. No. 33291), Adriane M. Antler (Reg. No. 32605), Thomas G. Rowan (Reg. No. 34419), James G. Markey (Reg. No. 31636), Thomas D. Kohler (Reg. No. 32797), Scott D. Stimpson (Reg. No. 33607), William S. Galliani (Reg. No. 33885), Gary S. Williams (Reg. No. 31066), Mark A. Farley (Reg. No. 33170) and Ann L. Gisolfi (Reg. No. 31956), all of Pennie & Edmonds LLP, whose addresses are 1155 Avenue of the Americas, New York, New York 10036, 1667 K Street N.W., Washington, DC 20006 and 3300 Hillview Avenue, Palo Alto, CA 94304, and each of them, my attorneys, to prosecute this application, and to transact all business in the Patent and Trademark Office connected therewith.

PENNIE & EDMONDS LLP DOCKET NO. 9740-069-999

SEND CORRESPONDENCE TO:	PENNIE & EDMONDS LLP 1155 Avenue of the Americas New York, N.Y. 10036-2711	DIRECT TELEPHONE CALLS TO: PENNIE & EDMONDS LLP DOCKETING (212) 790-2803

201	FULL NAME OF INVENTOR	LAST NAME SILVESTER	FIRST NAME Joseph	MIDDLE NAME	
	RESIDENCE & CITIZENSHIP	CITY Dollard-des-Ormeaux	STATE OR FOREIGN COUNTRY Québec	COUNTRY OF CITIZENSHIP CANADA	
	POST OFFICE ADDRESS	STREET 282 Place des Cèdres	CITY Dollard-des-Ormeaux	STATE OR COUNTRY CANADA	ZIP CODE H9G 1W1
202	FULL NAME OF INVENTOR	LAST NAME MILCZAREK ~~MALARCHUK~~ M	FIRST NAME Ed	MIDDLE NAME	
	RESIDENCE & CITIZENSHIP	CITY Pierrefonds	STATE OR FOREIGN COUNTRY Québec	COUNTRY OF CITIZENSHIP CANADA	
	POST OFFICE ADDRESS	STREET 5135 des Cajeux	CITY Pierrefonds	STATE OR COUNTRY CANADA	ZIP CODE H9J 3C4
203	FULL NAME OF INVENTOR	LAST NAME PETROGIANNIS	FIRST NAME Tommy	MIDDLE NAME	
	RESIDENCE & CITIZENSHIP	CITY Montréal	STATE OR FOREIGN COUNTRY Québec	COUNTRY OF CITIZENSHIP CANADA	
	POST OFFICE ADDRESS	STREET 4560 Cumberland Ave.	CITY Montréal Québec	STATE OR COUNTRY CANADA	ZIP CODE H4B 2L4
204	FULL NAME OF INVENTOR	LAST NAME	FIRST NAME	MIDDLE NAME	
	RESIDENCE & CITIZENSHIP	CITY	STATE OR FOREIGN COUNTRY	COUNTRY OF CITIZENSHIP	
	POST OFFICE ADDRESS	STREET	CITY	STATE OR COUNTRY	ZIP CODE
205	FULL NAME OF INVENTOR	LAST NAME	FIRST NAME	MIDDLE NAME	
	RESIDENCE & CITIZENSHIP	CITY	STATE OR FOREIGN COUNTRY	COUNTRY OF CITIZENSHIP	
	POST OFFICE ADDRESS	STREET	CITY	STATE OR COUNTRY	ZIP CODE
206	FULL NAME OF INVENTOR	LAST NAME	FIRST NAME	MIDDLE NAME	
	RESIDENCE & CITIZENSHIP	CITY	STATE OR FOREIGN COUNTRY	COUNTRY OF CITIZENSHIP	
	POST OFFICE ADDRESS	STREET	CITY	STATE OR COUNTRY	ZIP CODE

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issuing thereon.

SIGNATURE OF INVENTOR 201	SIGNATURE OF INVENTOR 202	SIGNATURE OF INVENTOR 203
DATE Sept 22, 1999	DATE Sept 23, 1999	DATE Sept 22 1999
SIGNATURE OF INVENTOR 204	SIGNATURE OF INVENTOR 205	SIGNATURE OF INVENTOR 206
DATE	DATE	DATE